**Обнаружение вируса и устранение последствий его влияния**

**Цель работы:** изучитьспособы обнаружения вирусов и устранение последствий их влияния

**Ход работы**

Классификация компьютерных вирусов

В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Так как подавляющее большинство современных вредительских программ обладают способностью к саморазмножению, то часто их относят к компьютерным вирусам. Все компьютерные вирусы могут быть классифицированы по следующим признакам:

* по среде обитания;
* по способу заражения;
* по степени опасности деструктивных (вредительских) воздействий;
* по алгоритму функционирования.

По среде обитания компьютерные вирусы делятся на:

* сетевые;
* файловые;
* загрузочные;
* комбинированные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. В отличие от резидентных нерезидентные вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

По степени опасности для информационных ресурсов пользователя компьютерные вирусы можно разделить на:

* безвредные вирусы;
* опасные вирусы;
* очень опасные вирусы.

Безвредные компьютерные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам КС. Ими, как правило, движет желание показать свои возможности программиста. Другими словами, создание компьютерных вирусов для таких людей - своеобразная попытка самоутверждения. Деструктивное воздействие таких вирусов сводится к выводу на экран монитора невинных текстов и картинок, исполнению музыкальных фрагментов и т. п.

К опасным относятся вирусы, которые вызывают существенное снижение эффективности КС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. Последствия таких вирусов могут быть ликвидированы без особых затрат материальных и временных ресурсов. Примерами таких вирусов являются вирусы, занимающие память ЭВМ и каналы связи, но не блокирующие работу сети; вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т. п.

Очень опасными следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию (в том числе и шифрование) информации, а также вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств и наносящие ущерб здоровью пользователям. Такие вирусы стирают отдельные файлы, системные области памяти, форматируют диски, получают несанкционированный доступ к информации, шифруют данные и т. п.

В соответствии с особенностями алгоритма функционирования вирусы можно разделить на два класса:

* вирусы, не изменяющие среду обитания (файлы и секторы) при распространении;
* вирусы, изменяющие среду обитания при распространении.

В свою очередь, вирусы, не изменяющие среду обитания, могут быть разделены на две группы:

* вирусы-"спутники" (соmраniоn);
* вирусы-"черви" (worm).

Вирусы-"спутники" не изменяют файлы. Механизм их действия состоит в создании копий исполняемых файлов.

Известны следующие методы обнаружения вирусов:

* сканирование;
* обнаружение изменений;
* эвристический анализ;
* использование резидентных сторожей;
* вакцинирование программ;
* аппаратно-программная защита от вирусов.

Сканирование - один из самых простых методов обнаружения вирусов. Сканирование осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса - сигнатуры.

Шаг 1. Выключить ЭВМ для уничтожения резидентных вирусов.



Шаг 2. Осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы.

Выбрать в биосе загрузку Windows с флешки. На флешку предварительно установить чистую ОС

Шаг 3. Сохранить на сменных носителях информации важные для вас файлы, которые не имеют резервных копий.

Так как есть доступ в жёсткий диск ПК, можно забрать все важные файлы. При этом не запуская вредоносные программы (вирусы).

Шаг 4. Использовать антивирусные средства для удаления вирусов и восстановления файлов.

Запуск антивирусного ПО

Шаг 5. Форматирование

Удалить все файлы и подозрительные ПО.

Шаг 6. Восстановить ОС.

После очистки вернуть все файлы из носителей

Шаг 7. Проверка восстановленных файлов

Тщательно проверить файлы, сохраненные после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы;

Шаг 8. Завершить восстановление информации всесторонней проверкой ЭВМ с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

**Вывод:** изучилспособы обнаружения вирусов и устранение последствий их влияния